Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Loblaw Companies Limited (Organization)
Decision number (file number)	P2017-ND-35 (File #005031)
Date notice received by OIPC	February 23, 2017
Date Organization last provided information	February 23, 2017
Date of decision	February 24, 2017
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address (street, city, province, postal code), • telephone number, • date of birth (and/or year), • email address, • security question and answer, • meal preference information, and • transaction information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some or all of the information about Albertans was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization operates a points rewards loyalty program known as PC Plus. • On December 9, 2016, the Organization received several calls from PC Plus members concerning the disappearance of rewards points from their membership accounts. • The Organization's investigation confirmed member accounts had been targeted by threat actors operating in the Internet "dark web". It appears fraudulent redemption of points began December 1, 2016. • The Organization believes member accounts were accessed using usernames and/or passwords stolen from other sites.
Affected individuals	A total of 55,406 individuals were affected, including 6,991 in Alberta.
Steps taken to reduce risk of harm to individuals	• Initiated an internal investigation, as well as an independent cyber-forensics investigation. • Reported the incident to law enforcement, which resulted in a number of arrests. • Froze points redemption on accounts, forced password resets, and implemented a number of enhanced security measures (including improved authentication).
Steps taken to notify individuals of the incident	Affected individuals were notified in a variety of ways, including by telephone and email, and in a notice sent February 20-21, 2017.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported that it believes "the primary purpose of this activity is to commit fraud against [the Organization]"; however, identity theft and "risk of increased phishing attempts" were identified as possible harms that might result to affected individuals from this incident. I agree with the Organization's assessment. Identity (date of birth), contact and profile information could be used to cause the harms of identity theft and fraud. Credentials (security question and answer) and email addresses could be used to gain unauthorized access to other internet accounts and could be used for phishing purposes. These are significant harms.

Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported "it believes that the risk of harm may be enough to reach the threshold where there is a real risk of significant harm to the affected individuals." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious action (deliberate intrusion) and has not been recovered. Further, the information has been used for fraudulent purposes.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals. Identity, contact and profile information could be used to cause the harms of identity theft and fraud. Credentials (security question and answer) and email addresses could be used to gain unauthorized access to other internet accounts and could be used for phishing purposes. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious action (deliberate intrusion) and has not been recovered. Further, the information has been used for fraudulent purposes.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals in a variety of ways, including by telephone, and email, and in a notice sent February 20-21, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner